UNITED STATES PATENT AND TRADEMARK OFFICE

**UNITED STATES DEPARTMENT OF COMMERCE**
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/893,523 | 06/29/2001 | Rickard Nelger | 1076.40323X00 | 2984 |

20457 7590 07/01/2005

ANTONELLI, TERRY, STOUT & KRAUS, LLP
1300 NORTH SEVENTEENTH STREET
SUITE 1800
ARLINGTON, VA 22209-3873

| EXAMINER | |
|---|---|
| SHANNON, MICHAEL R | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2614 | |

DATE MAILED: 07/01/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

| | | |
|---|---|---|
| ***Office Action Summary*** | **Application No.**<br>09/893,523 | **Applicant(s)**<br>NELGER ET AL. |
| | **Examiner**<br>Michael R. Shannon | **Art Unit**<br>2614 |

***-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --***

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *29 June 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 June 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 102*

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-7, 10-12, 15-16, 18-24, and 26-28 are rejected under 35 U.S.C. 102(b) as being anticipated by Gammie (USP 5,029,207), cited by examiner.

Regarding claim 1, the claimed "conditional access system" is met as follows:

- The claimed "first transmitter for transmitting a scrambled broadcast stream" is met by satellite link 505 of Figure 5, which is used for transmitting the scrambled broadcast stream. Figure 5 shows an example of the case wherein the key (ECM) is transmitted along with the broadcast signal. However, figure 9 and column 1, lines 63 – column 2, line 12, teach that this does not have to be the case and in fact the key could be transmitted over an alternate data channel.
- The claimed "second transmitter for transmitting a plurality of control messages separate from the broadcast stream, said control messages including information for descrambling the broadcast stream" is met by the key being sent over a separate data channel "out-of-band" or even over a telephone line [col. 2, lines 10-12], as pictured in Figure 9 from the head-end 501 to the receiver 506.

Regarding claim 2, the claimed “conditional access system according to claim 1, wherein said control messages are alone sufficient to permit the broadcast stream to be descrambled” is met by the fact that the key is used alone to descramble the scrambled content [col. 1, lines 55-57], note the lack of smart card in figure 5. Once the key is delivered via the satellite connection or the separate data channel, the key is used directly to descramble the scrambled program.

Regarding claim 3, the claimed " conditional access system according to claim 1, wherein said information for descrambling the broadcast stream is incorporated into each of said control messages without being encrypted” is met by the fact that the key may or may not itself be encrypted [col. 1, lines 51-52]. As in prior art systems pictures in Figure 1, the key is not encrypted before transmission.

Regarding claim 4, the claimed “conditional access system according to claim 1, wherein said information for descrambling the broadcast stream is encrypted prior to being incorporated into each of said control messages” is met by the fact that the key may itself be encrypted prior to transmission (be it multiplexed with the signal or over a dedicated separate data channel) [col. 1, lines 51-52]. The key encryptor 510 of figure 5 can serve to encrypt the key prior to transmission.

Regarding claim 5, the claimed “conditional access system according to claim 1, further comprising a scrambler and a key generator for generating a stream of encryption keys, the scrambler being operable to encrypt a broadcast stream with the encryption key stream, the system further being operable to send the encryption key stream to a decoder for decoding the encrypted broadcast stream, said encrypted key stream comprising the information for descrambling the broadcast stream" is met as follows: The scrambler is met by the Program Scrambler 503 and the key generator is met by the Key Memory 504, and Database 511, which serve to create a key for descrambling the program (usually a new key is created on a regular basis such as monthly to discourage piracy) [col. 2, lines 40-41]. The scrambler is able to use the key in order to encrypt and scramble the program in the program scrambler 503 before transmission. The key is then sent to the Decoder 506 via a satellite link 505 or separate data channel [col. 2, lines 10-12] and decrypted at decryptors 513 of Figure 5. The decrypted key is then used to descramble the program in the program descrambler 508.

Regarding claim 6, the claimed "conditional access system according to claim 1, wherein the second transmitter is arranged to transmit the descrambling information to a receiver using a point-to-point protocol" is met by the fact that a telephone line could be used to transmit the key to the decoder [col. 2, lines 10-12].

Regarding claim 7, the claimed "conditional access system according to claim 1, wherein the second transmitter is arranged to transmit the descrambling information over a secure connection" is met by the same fact that a telephone line could be used to transmit the key to the decoder [col. 2, lines 10-12], which, inherently, is secure, since it is a point-to-point transmission.

Regarding claim 10, the claimed "conditional access system" is met as follows:

- The claimed "first receiver for receiving a scrambled broadcast stream" is met by the reception of the satellite link 505 of Figure 5, which is used to receive the scrambled broadcast stream. Figure 5 shows an example of the case wherein the key (ECM) is transmitted along with the broadcast signal. However, figure 9 and column 1, lines 63 – column 2, line 12, teach that this does not have to be the case and in fact the key could be transmitted over an alternate data channel.

- The claimed "second receiver for receiving a plurality of control messages separate from the broadcast stream, the control messages including information for descrambling the broadcast stream" is met by the key being received over a separate data channel "out-of-band" or even over a telephone line [col. 2, lines 10-12], as pictured in Figure 9 from the head-end 501 to the receiver 506.

Regarding claim 11, the claimed "conditional access system according to claim 10, wherein the control messages are sent to the second receiver using a point-to-point protocol" is met by the fact that a telephone line could be used to transmit the key to the decoder [col. 2, lines 10-12].

Regarding claim 12, the claimed "conditional access system according to claim 10, wherein the control messages are sent to the second receiver over a secure connection" is met by the same fact that a telephone line could be used to transmit the key to the decoder [col. 2, lines 10-12], which, inherently, is secure, since it is a point-to-point transmission.

Regarding claim 15, the claimed "conditional access system according to claim 10, further comprising a decoder for descrambling the broadcast stream in accordance with the descrambling information" is met by the program descrambler 508, which serves to descramble the received scrambled program using the received key [col. 12, lines 31-34].

Regarding claim 16, the claimed "conditional access system according to claim 10, wherein said information for descrambling the broadcast stream is incorporated into said control messages without being encrypted, whereby the decoder does not require a smart card for decryption" is met by the fact that the key may or may not itself be encrypted [col. 1, lines 51-52] and by the fact that the key is used alone to descramble the scrambled content [col. 1, lines 55-57], note the lack of smart card in figure 5. Once the key is delivered via the satellite connection or the separate data channel, the key is used directly to descramble the scrambled program. As in prior art systems pictures in Figure 1, the key is not encrypted before transmission.

Regarding claim 18, the claimed "decoder for use in a conditional access system for decrypting encrypted broadcast content" is met as follows:

- The claimed "first input module for receiving said encrypted broadcast content from a first communications channel" is met by the reception of the satellite link 505 of Figure 5, which is used to receive the scrambled broadcast stream. Figure 5 shows an example of the case wherein the key (ECM) is transmitted along with the broadcast signal. However, figure 9 and column 1, lines 63 – column 2, line 12, teach that this does not have to be the case and in fact the key could be transmitted over an alternate data channel.

- The claimed "second input module for receiving a plurality of control messages from a second communications channel, said control messages containing descrambling information for decrypting said broadcast content" is met by the key being received over a separate data channel "out-of-band" or even over a telephone line [col. 2, lines 10-12], as pictured in Figure 9 from the head-end 801 to the receiver 806.

Regarding claim 19, the claimed "decoder according to claim 18, further comprising a processor module for extracting said descrambling information from said control messages" is met by the key decryptor 513, which serves to decrypt the received key and use it for descrambling the program.

Regarding claim 20, the claimed "decoder according to claim 19, further comprising a descrambler for receiving said encrypted broadcast content and decrypting said content using said descrambling information" is met by the program descrambler 508, which serves to descramble the received scrambled program using the received key [col. 12, lines 31-34].

Regarding claim 21, the claimed "method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a decoder, said decoder being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising sending said control messages to said decoder separately from said broadcast stream" is met by the satellite link 505 of Figure 8, which is used for transmitting the scrambled broadcast stream. Figure 5 shows an example of the case wherein the key (ECM) is transmitted along with the broadcast signal. However, figure 9 and column 1, lines 63 – column 2, line 12, teach that this does not have to be the case and in fact the key could be transmitted over an alternate data channel. Furthermore, the key can be sent over a separate data channel "out-of-band" or even over a telephone line [col. 2, lines 10-12], as pictured in Figure 9 from the head-end 801 to the receiver 806.

Regarding claim 22, the claimed "method according to claim 21, comprising incorporating said descrambling information into the control messages without encrypting it" is met by the fact that the key may or may not itself be encrypted [col. 1, lines 51-52]. As in prior art systems pictures in Figure 1, the key is not encrypted before transmission.

Regarding claim 23, the claimed "method according to claim 22, comprising encrypting the control messages prior to sending them to the decoder" is met by the fact that the key may itself be encrypted prior to transmission (be it multiplexed with the signal or over a dedicated separate data channel) [col. 1, lines 51-52]. The key encryptor 510 of figure 5 can serve to encrypt the key prior to transmission.

Regarding claim 24, the claimed "method according to claim 21, comprising sending the control message over a secure channel" is met by the fact that a telephone line could be used to transmit the key to the decoder [col. 2, lines 10-12], which, inherently, is secure, since it is a point-to-point transmission.

Regarding claim 26, the claimed "method for use in a conditional access system, in which a scrambled broadcast stream is transmitted to a first decoder and a second decoder, said first and second decoders being operable to receive a plurality of control messages including information for descrambling the broadcast stream, the method comprising receiving a request to transmit a plurality of control messages to said second decoder separately from the broadcast stream" is met by the satellite link 505 of Figure 5, which is used for transmitting the scrambled broadcast stream to multiple receivers 506. Figure 5 shows an example of the case wherein the key (ECM) is transmitted along with the broadcast signal. However, figure 9 and column 1, lines 63 – column 2, line 12, teach that this does not have to be the case and in fact the key could be transmitted over an alternate data channel. Column 1, lines 57-62 teach that an unauthorized user is denied access to the key so that he/she cannot descramble the received program. The encrypted key can be addressed to individual decoders upon request [col. 9, line 68 – col. 10, line 2].

Regarding claim 27, the claimed "method according to claim 26, wherein said control messages are alone sufficient to descramble said broadcast stream" is met by the fact that the key is used alone to descramble the scrambled content [col. 1, lines 55-57], note the lack of smart card in figure 5. Once the key is delivered via the satellite connection or the separate data channel, the key is used directly to descramble the scrambled program.

Regarding claim 28, the claimed "method according to claim 26, further comprising denying a service to the first decoder while the plurality of control messages is being sent to the second decoder" is met by Column 1, lines 57-62, wherein Gammie teaches that an unauthorized user is denied access to the key so that he/she cannot descramble the received program.

## *Claim Rejections - 35 USC § 103*

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 8, 13, 17, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gammie (USP 5,029,207), cited by examiner.

Regarding claim 8, the Gammie reference teaches all of that which is discussed above with regards to claim 7. The Gammie reference does not, however, disclose the use of a virtual private network (VPN) for implementing the secure connection. The examiner takes OFFICIAL NOTICE that it is notoriously well known in the art to implement highly secure and encrypted connections for the transmission of sensitive content using VPNs. Gammie even suggests the use of an encrypted separate data channel for the transmission of the descrambling key [col. 2, lines 10-12]. Therefore, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to utilize a VPN for transmission of the encoded descrambling key, in order to use a highly secure connection that would discourage piracy and hacking.

Regarding claim 13, the Gammie reference teaches all of that which is discussed above with regards to claim 12. The Gammie reference does not, however, disclose the use of a virtual private network (VPN) for implementing the secure connection. The examiner takes OFFICIAL NOTICE that it is notoriously well known in the art to implement highly secure and encrypted connections for the transmission of sensitive content using VPNs. Gammie even suggests the use of an encrypted separate data channel for the transmission of the descrambling key [col. 2, lines 10-12]. Therefore, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to utilize a VPN for transmission of the encoded descrambling key, in order to use a highly secure connection that would discourage piracy and hacking.

Regarding claim 17, the Gammie reference teaches all of that which is discussed above with regards to claim 10. The Gammie reference does not, however, disclose that the second receiver comprises a mobile telephone. The Gammie reference does disclose the use of a telephone connection to implement a separate data channel for the transmission of the descrambling key [col. 2, lines 10-12]. The examiner takes OFFICIAL NOTICE that it is notoriously known in the art to use mobile phones for communication in place of a regular telephone. Therefore, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to use a mobile telephone in place of the suggested telephone, in order to create a separate data channel for the transmission of the descrambling key information.

Regarding claim 25, the Gammie reference teaches all of that which is discussed above with regards to claim 24. The Gammie reference does not, however, disclose the use of a virtual private network (VPN) for implementing the secure connection. The examiner takes OFFICIAL NOTICE that it is notoriously well known in the art to implement highly secure and encrypted connections for the transmission of sensitive content using VPNs. Gammie even suggests the use of an encrypted separate data channel for the transmission of the descrambling key [col. 2, lines 10-12]. Therefore, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to utilize a VPN for transmission of the encoded descrambling key, in order to use a highly secure connection that would discourage piracy and hacking.

5. Claims 9, 14, and 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gammie (USP 5,029,207) in view of Wasilewski et al (USP 6,157,719), both cited by examiner.

Regarding claim 9, the Gammie reference teaches all of that which is discussed above with regards to claim 1. The Gammie reference does not expressly disclose that the control message comprises an entitlement control message (ECM). While the Gammie reference does disclose the ability to send the descrambling key over an alternative data channel, it does not disclose that the descrambling key is an ECM. The Wasilewski reference discloses the general conditional access system overview, wherein an ECM is used to decrypt the encrypted program [col. 4, lines 27-33]. Further, the Wasilewski reference discloses encrypted EMMs (entitlement management messages), which could be sent over a separate channel [col. 5, lines 6-14]. In view of the Wasilewski reference, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to use ECMs as a way to send and package the descrambling keys, in order to utilize a technology that is commonly used and accepted in the conditional access art. As suggested by the Wasilewski reference, ECMs can contain information (a key) used for decrypting the encrypted program [col. 4, lines 27-33].

Regarding claim 14, the Gammie reference teaches all of that which is discussed above with regards to claim 10. The Gammie reference does not expressly disclose that the control message comprises an entitlement control message (ECM). While the Gammie reference does disclose the ability to send the descrambling key over an alternative data channel, it does not disclose that the descrambling key is an ECM. The Wasilewski reference discloses the general conditional access system overview, wherein an ECM is used to decrypt the encrypted program [col. 4, lines 27-33]. Further, the Wasilewski reference discloses encrypted EMMs (entitlement management messages), which could be sent over a separate channel [col. 5, lines 6-14]. In view of the Wasilewski reference, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to use ECMs as a way to send and package the descrambling keys, in order to utilize a technology that is commonly used and accepted in the conditional access art. As suggested by the Wasilewski reference, ECMs can contain information (a key) used for decrypting the encrypted program [col. 4, lines 27-33].

Regarding claim 29, the claimed "conditional access system" is met as follows:

- The claimed "first communication channel for carrying a broadcast stream, said stream being scrambled with a stream of control words" is met by the Gammie reference, wherein the satellite link 505 of Figure 5, is used for transmitting the scrambled broadcast stream. The stream being scrambled using a stream of control words is met by the basic conditional access system overview taught by Wasilewski, wherein a control word stream is used to scramble the elementary stream to create the scrambled program stream [col. 6, lines 37-44]. It would have been obvious to one of ordinary skill in the art to scramble the broadcast stream of Gammie using a control word stream, in order to adhere to commonly accepted scrambling practices such as that taught by Wasilewski.

- The claimed "second communications channel separate from the first channel for carrying a stream of entitlement control messages, said entitlement control messages incorporating information relating to the stream of control words for descrambling the broadcast stream" is met by the Gammie reference, wherein Gammie discloses the ability to send the descrambling key over an alternative data channel. However, Gammie does not disclose that the descrambling key is an ECM. The Wasilewski reference discloses the general conditional access system overview, wherein an ECM is used to decrypt the encrypted program [col. 4, lines 27-33]. Further, the Wasilewski reference discloses encrypted EMMs (entitlement management messages), which could be sent over a separate channel [col. 5, lines 6-14]. In view of the Wasilewski reference, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to use ECMs as a way

> to send and package the descrambling keys over a separate communications channel, in order to utilize a technology that is commonly used and accepted in the conditional access art. As suggested by the Wasilewski reference, ECMs can contain information (a key) used for decrypting the encrypted program [col. 4, lines 27-33].

Regarding claim 30, the Gammie and Wasilewski references teach all of that which is discussed above with regards to claim 29. The Gammie reference does not teach that the "entitlement control messages alone contain all of the information required to descramble the broadcast stream". The Gammie reference does teach that the key transmitted over the separate data channel [col. 2, lines 10-12] alone is enough to decrypt/descramble the program [col. 1, lines 55-57], note the lack of smart card in figure 5. Once the key is delivered via the satellite connection or the separate data channel, the key is used directly to descramble the scrambled program. However, Gammie does not disclose that the descrambling key is an ECM. The Wasilewski reference discloses the general conditional access system overview, wherein an ECM is used to decrypt the encrypted program [col. 4, lines 27-33]. Further, the Wasilewski reference discloses encrypted EMMs (entitlement management messages), which could be sent over a separate channel [col. 5, lines 6-14]. In view of the Wasilewski reference, the examiner submits that it would have been clearly obvious to one of ordinary skill in the art at the time of the invention to use ECMs as a way to send and package the descrambling keys over a separate communications channel, in order to utilize a technology that is commonly used and accepted in the conditional access art.

As suggested by the Wasilewski reference, ECMs can contain information (a key) used for decrypting the encrypted program [col. 4, lines 27-33].

### *Conclusion*

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Son et al (USP 6,229,895) disclose a system for secure distribution of video-on-demand. Note column 5, lines 29-35, wherein Son discloses that the private key may be transported from the source to the server via a communication channel which is separate from the communication channel used to transport the video program from the source to the server.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R. Shannon who can be reached at (571) 272-7356 or Michael.Shannon@uspto.gov. The examiner can normally be reached by phone Monday through Friday 8:00 AM – 5:00PM, with alternate Friday's off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Miller, can be reached at (571) 272-7353.

**Any response to this action should be mailed to:**

Please address mail to be delivered by the United States Postal Service (USPS) as follows:

Mail Stop _______
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Effective January 14, 2005, except correspondence for Maintenance Fee payments, Deposit Account Replenishments (see 1.25(c)(4)), and Licensing and Review (see 37 CFR 5.1(c) and 5.2(c)), please address correspondence to be delivered by other delivery services (Federal Express (Fed Ex), UPS, DHL, Laser, Action, Purolater, etc.) as follows:

United States Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Some correspondence may be submitted electronically. See the Office's Internet Web site http://www.uspto.gov for additional information.

**Or faxed to: (571) 273-8300**

**Hand-delivered responses should be brought to**:

Randolph Building
401 Dulany Street
Alexandria, VA 22314

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to customer service whose telephone number is **(571) 272-2600**.

Michael R Shannon
Examiner
Art Unit 2614

Michael R. Shannon
June 23, 2005

JOHN MILLER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600